ONTAP tools for VMware vSphere 구성

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

목차

ONTAP tools for VMware vSphere 구성

vCenter Server 인스턴스를 ONTAP tools에 추가합니다

vCenter Server 인스턴스를 ONTAP tools for VMware vSphere에 추가하여 vCenter Server 환경의 가상 데이터 저장소를 구성, 관리 및 보호할 수 있습니다. 여러 vCenter Server 인스턴스를 추가하는 경우 ONTAP tools와 각 vCenter Server 간의 안전한 통신을 위해 사용자 지정 CA 인증서가 필요합니다.

이 작업 정보

ONTAP tools는 vCenter Server와 통합되어 vSphere 클라이언트에서 직접 프로비저닝, 스냅샷 및 데이터 보호와 같은 스토리지 작업을 수행할 수 있습니다.

vCenter Server 인스턴스를 ONTAP tools에 추가하면 다음과 같은 작업이 자동으로 실행됩니다.

- ONTAP tools는 vCenter 클라이언트 플러그인을 원격 플러그인으로 등록합니다.
- 플러그인 및 API에 대한 사용자 지정 권한은 vCenter Server 인스턴스에 적용됩니다.
- 사용자 관리를 위해 사용자 지정 역할을 생성합니다.
- 해당 플러그인은 vSphere 사용자 인터페이스에 바로 가기로 표시됩니다.

시작하기 전에

- vCenter Server 인증서에 DNS 및 IP 주소 항목이 모두 포함된 유효한 SAN(Subject Alternative Name) 확장이 있는지 확인하십시오. 예를 들면 다음과 같습니다.

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  인증서에 SAN 확장이 포함되어 있지 않거나 SAN 확장에 올바른 DNS 또는 IP 주소 값이 포함되어 있지 않은 경우 인증서 유효성 검사 오류로 인해 ONTAP tools 작업이 실패할 수 있습니다.

- vCenter Server의 Primary Network Identifier(PNID)는 SAN 세부 정보에 포함되어야 합니다. PNID와 DNS 이름은 동일해야 하며 DNS에서 확인 가능해야 합니다.
- vCenter Server를 배포할 때는 정규화된 도메인 이름(FQDN)을 사용하는 것이 좋습니다. 최적의 호환성과 지원을 위해 인증서의 SAN에 DNS Name=machine_FQDN이 포함되어 있는지 확인하십시오.
- 자세한 내용은 VMware 설명서를 참조하십시오.
  - "vSphere 다양한 솔루션 경로에 대한 인증서 요구 사항"
  - "vCenter 머신 SSL 인증서 교체 사용자 지정 인증 기관 서명 인증서"
  - "오류: Subject Alternate Name(SAN) 필드에 PNID가 없습니다. 유효한 인증서를 제공하십시오"

FQDN을 사용할 수 없는 경우 PNID를 IP 주소로 설정하고 해당 IP 주소를 SAN에 포함할 수 있습니다. 하지만 VMware에서는 이 방법을 권장하지 않습니다.

단계

1. 웹 브라우저를 열고 다음 URL로 이동하세요: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. **vCenters** > *추가*를 선택하여 vCenter Server 인스턴스를 온보딩합니다. vCenter IP 주소 또는 호스트 이름, 사용자 이름, 암호 및 포트 세부 정보를 입력합니다.
4. 고급 옵션에서 vCenter Server 인증서를 자동으로 가져오거나(인증) 수동으로 업로드할 수 있습니다.

ONTAP tools에 vCenter 인스턴스를 추가하는 데 관리자 계정이 필요하지 않습니다. 관리자 계정 없이도 제한된 권한을 가진 사용자 지정 역할을 생성할 수 있습니다. 자세한 내용은 "vCenter Server RBAC와 ONTAP tools for VMware vSphere 10 함께 사용하기"을 참조하십시오.

ONTAP 도구에서 VASA Provider를 vCenter Server 인스턴스에 등록합니다

ONTAP tools for VMware vSphere를 사용하여 VASA Provider를 vCenter Server 인스턴스에 등록하십시오. 이를 통해 스토리지 정책 기반 관리, vVols 지원 및 ONTAP 시스템에서 VMware Live Site Recovery 어플라이언스와의 통합이 가능해집니다.

VASA 공급자 설정에는 선택한 vCenter Server의 등록 상태가 표시됩니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > *NetApp ONTAP tools*를 선택하십시오.
3. 설정 > *VASA 공급자 설정*을 선택합니다. ONTAP tools에서 VASA Provider 등록 상태가 등록되지 않음으로 표시됩니다.
4. VASA 제공업체를 등록하려면 등록 버튼을 선택하십시오.
5. VASA Provider의 이름과 자격 증명을 입력하십시오. 사용자 이름에는 문자, 숫자 및 밑줄만 사용할 수 있습니다. 비밀번호는 8자에서 256자 사이여야 합니다.
6. *등록*을 선택합니다.
7. 등록이 성공적으로 완료되고 페이지가 새로고침되면 ONTAP tools는 등록된 VASA Provider의 상태, 이름 및 버전을 표시합니다.

다음 단계

vCenter 클라이언트에서 온보딩된 VASA Provider가 VASA Provider 목록에 표시되는지 확인하십시오.

단계

1. vCenter Server 인스턴스로 이동합니다.
2. 관리자 자격 증명으로 로그인합니다.
3. **Storage Providers** > *구성*을 선택합니다. 등록된 VASA Provider가 목록에 올바르게 표시되는지 확인합니다.

ONTAP tools를 사용하여 NFS VAAI 플러그인 설치

NFS vStorage API for Array Integration(NFS VAAI) 플러그인은 VMware vSphere를 NFS 스토리지 어레이에 연결합니다. ONTAP tools for VMware vSphere를 사용하여 VAAI 플러그인을 설치하십시오. 이를 통해 ESXi 호스트 대신 NFS 스토리지 어레이에서 특정 스토리지 작업을 처리할 수 있습니다.

시작하기 전에

- "NetApp VMware VAAI용 NFS 플러그인" 설치 패키지를 다운로드하십시오.
- vSphere 7.0 U3(최신 패치 이상) 및 ONTAP 9.14.1 이상이 설치된 ESXi 호스트가 있는지 확인하십시오.
- NFS 데이터 저장소를 마운트합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션에서 바로가기 > *NetApp ONTAP tools*를 선택하십시오.
3. 설정 > *NFS VAAI 도구*를 선택합니다.
4. 이미 VAAI 플러그인을 vCenter Server에 업로드한 경우 *기존 버전*에서 *변경*을 선택하십시오. 업로드하지 않은 경우 *업로드*를 선택하십시오.
5. `.vib` 파일을 찾아 선택한 다음 *업로드*를 선택하여 ONTAP tools에 파일을 업로드하십시오.
6. *ESXi 호스트에 설치*를 선택하고 NFS VAAI 플러그인을 설치할 ESXi 호스트를 선택한 다음 *설치*를 선택합니다.

   vSphere 웹 클라이언트에는 플러그인을 설치할 수 있는 ESXi 호스트만 표시됩니다. 최근 작업 섹션에서 설치 진행 상황을 모니터링할 수 있습니다.

7. 설치 후 ESXi 호스트를 수동으로 재시작하십시오.

   ESXi 호스트를 재시작하면 ONTAP tools for VMware vSphere에서 NFS VAAI 플러그인을 자동으로 감지하고 활성화합니다.

다음 단계

NFS VAAI 플러그인을 설치하고 ESXi 호스트를 재부팅한 후 VAAI 복사 오프로드를 위한 NFS 내보내기 정책을 구성하십시오. 내보내기 정책 규칙이 다음 요구 사항을 충족하는지 확인하십시오.

- 해당 ONTAP 볼륨은 NFSv4 호출을 허용합니다.
- 루트 사용자는 루트 권한을 유지하며 모든 접합 상위 볼륨에서 NFSv4가 허용됩니다.
- VAAI 지원 옵션은 해당 NFS 서버에 설정됩니다.

자세한 내용은 "VAAI 복사 오프로드를 위해 올바른 NFS 내보내기 정책을 구성합니다"KB 문서를 참조하십시오.

관련 정보

"NFS를 통한 VMware vStorage 지원"

"NFSv4.0 활성화 또는 비활성화"

"ONTAP의 NFSv4.2 지원"

ONTAP tools에서 ESXi 호스트 설정을 구성합니다.

ESXi 서버의 다중 경로 및 타임아웃 설정을 구성하면 데이터 가용성과 무결성을 유지하는 데 도움이 됩니다. 기본 경로를 사용할 수 없게 될 경우 백업 스토리지 경로로 자동 페일오버가 가능합니다.

ESXi 서버 다중 경로 및 타임아웃 설정 구성

ONTAP tools for VMware vSphere는 NetApp 스토리지 시스템과 가장 잘 호환되는 ESXi 호스트 다중 경로 설정 및 HBA 타임아웃 설정을 확인하고 설정합니다.

이 작업 정보

이 과정은 사용자의 설정 및 시스템 부하에 따라 시간이 걸릴 수 있습니다. 진행 상황은 최근 작업 패널에서 확인할 수 있습니다.

단계

1. VMware vSphere 웹 클라이언트 홈 페이지에서 *호스트 및 클러스터*를 선택합니다.
2. VMware vSphere 웹 클라이언트의 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. ONTAP tools for VMware vSphere 플러그인의 개요(대시보드)에서 **ESXi** 호스트 규정 준수 카드로 이동합니다.
4. 권장 설정 적용 링크를 선택합니다.
5. 권장 호스트 설정 적용 창에서 NetApp 권장 설정을 사용하도록 업데이트할 호스트를 선택하고 *다음*을 선택합니다.

   ⓘ ESXi 호스트를 확장하면 현재 값을 확인할 수 있습니다.

6. 설정 페이지에서 필요에 따라 권장 값을 선택하십시오.
7. 요약 창에서 값을 확인하고 *완료*를 선택합니다. 최근 작업 패널에서 진행 상황을 확인할 수 있습니다.

ESXi 호스트 값 설정

ONTAP tools for VMware vSphere를 사용하여 ESXi 호스트의 시간 초과 및 기타 값을 설정하여 최적의 성능과 장애 조치를 구현할 수 있습니다. 이러한 값은 NetApp 테스트를 기반으로 설정됩니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

HBA/CNA 어댑터 설정

다음 매개변수를 기본값으로 설정합니다.

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA 타임아웃
- QLogic FC HBA 타임아웃

MPIO 설정

MPIO 설정은 NetApp 스토리지 시스템에 가장 적합한 경로를 선택합니다. MPIO 설정은 최적의 경로를 선택하고 이를 사용합니다.

고성능 환경이나 단일 LUN 데이터스토어를 사용한 테스트 시에는 라운드 로빈(VMW_PSP_RR) 경로 선택 정책(PSP)의 로드 밸런싱 설정을 조정하여 성능을 향상시킬 수 있습니다. 기본 IOPS 값을 1000에서 1로 설정하십시오.

MPIO 설정은 NVMe, NVMe/FC 및 NVMe/TCP 프로토콜에는 적용되지 않습니다.

NFS 설정

매개변수	이 값을 …로 설정하십시오.
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 이상
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

ONTAP tools에 대한 ONTAP 사용자 역할 및 권한을 구성합니다

이 섹션을 사용하여 ONTAP tools for VMware vSphere 및 ONTAP System Manager를 사용하는 스토리지 백엔드에 대한 ONTAP 사용자 역할 및 Privileges를 구성하십시오. 제공된 JSON 파일을 사용하여 역할을 할당하거나, 사용자 및 역할을 수동으로 생성하거나, 관리자가 아닌 계정에 필요한 최소 Privileges를 적용할 수 있습니다.

시작하기 전에

- _\https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip_을 사용하여 ONTAP tools for VMware vSphere에서 ONTAP Privileges 파일을 다운로드하십시오. zip 파일을 다운로드하면 두 개의 JSON 파일이 있습니다. ASA r2 시스템을 구성할 때는 ASA r2 전용 JSON 파일을 사용하십시오.

  클러스터 수준 또는 스토리지 가상 머신(SVM) 수준에서 직접 사용자를 생성할 수 있습니다. user_roles.json 파일을 사용하지 않는 경우, 사용자에게 필요한 최소 SVM 권한이 부여되었는지 확인하십시오.

- 스토리지 백엔드에 대한 관리자 권한으로 로그인하십시오.

단계

1. 다운로드한 *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* 파일의 압축을 푸세요.
2. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스하십시오.

3. 관리자 권한으로 클러스터에 로그인합니다. 사용자를 구성하려면 다음을 수행합니다.
   a. 클러스터 ONTAP tools 사용자를 구성하려면 클러스터 > 설정 > 사용자 및 역할 창을 선택하십시오.
   b. SVM ONTAP tools 사용자를 구성하려면 스토리지 **SVM** > 설정 > 사용자 및 역할 창을 선택하십시오.
   c. 사용자 아래에서 *추가*를 선택합니다.
   d. 사용자 추가 대화 상자에서 *가상화 제품*을 선택합니다.
   e. 찾아보기 를 사용하여 ONTAP Privileges JSON 파일을 선택하고 업로드하십시오. ASA r2 이외의 시스템에서는 users_roles.json 파일을 선택하고, ASA r2 시스템에서는 users_roles_ASAr2.json 파일을 선택하십시오.

      ONTAP tools는 제품 필드를 자동으로 채웁니다.

   f. 드롭다운 메뉴에서 제품 기능을 *VSC, VASA Provider 및 SRA*로 선택하십시오.

      ONTAP tools는 사용자가 선택한 제품 기능에 따라 역할 필드를 자동으로 채웁니다.

   g. 필수 사용자 이름과 비밀번호를 입력합니다.
   h. 사용자에게 필요한 Privileges(Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role)를 선택한 다음 *추가*를 선택합니다.

ONTAP tools가 새 역할과 사용자를 추가합니다. 구성한 역할에 대한 Privileges를 확인할 수 있습니다.

SVM 애그리게이트 매핑 요구 사항

SVM 사용자 자격 증명을 사용하여 데이터스토어를 프로비저닝할 때, ONTAP tools for VMware vSphere는 데이터스토어 POST API에 지정된 애그리게이트에 볼륨을 생성합니다. ONTAP는 SVM 사용자가 SVM에 매핑되지 않은 애그리게이트에 볼륨을 생성하는 것을 방지합니다. 볼륨을 생성하기 전에 ONTAP REST API 또는 CLI를 사용하여 SVM을 필요한 애그리게이트에 매핑하십시오.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

ONTAP 사용자 및 역할을 수동으로 생성

JSON 파일 없이 수동으로 사용자 및 역할을 생성합니다.

1. 클러스터의 클러스터 관리 IP 주소를 사용하여 ONTAP System Manager에 액세스하십시오.
2. 관리자 권한으로 클러스터에 로그인합니다.
   a. 클러스터 ONTAP tools 역할을 구성하려면 클러스터 > 설정 > *사용자 및 역할*을 선택하십시오.
   b. 클러스터 SVM ONTAP tools 역할을 구성하려면 스토리지 **SVM** > 설정 > *사용자 및 역할*을 선택하십시오.
3. 역할 생성:
   a. 역할 테이블에서 *추가*를 선택합니다.
   b. 역할 이름 및 역할 속성 세부 정보를 입력합니다.

      *REST API 경로*를 추가하고 드롭다운 목록에서 액세스 권한을 선택합니다.

   c. 필요한 API를 모두 추가하고 변경 사항을 저장합니다.
4. 사용자 생성:
   a. 사용자 테이블에서 *추가*를 선택합니다.
   b. 사용자 추가 대화 상자에서 *System Manager*를 선택합니다.
   c. *사용자 이름*을 입력하세요.
   d. 위의 역할 생성 단계에서 생성된 옵션 중에서 *역할*을 선택합니다.
   e. 액세스 권한을 부여할 애플리케이션과 인증 방법을 입력합니다. ONTAPI와 HTTP는 필수 애플리케이션이며, 인증 유형은 *Password*입니다.
   f. *사용자 비밀번호*를 설정하고 사용자를 *저장*합니다.

관리자 권한이 없는 전역 범위 클러스터 사용자에게 필요한 최소 권한 목록

이 페이지는 JSON 파일 없이 관리자 권한이 없는 전역 범위 클러스터 사용자에게 필요한 최소 권한을 나열합니다. 클러스터가 로컬 범위에 있는 경우 ONTAP tools for VMware vSphere는 ONTAP에서 프로비저닝하기 위해 읽기 권한 이상이 필요하므로 JSON 파일을 사용하여 사용자를 생성하십시오.

API를 사용하여 기능에 액세스할 수 있습니다.

API	액세스 수준	사용 대상
/api/cluster	읽기 전용	클러스터 구성 검색
/api/cluster/licensing/licenses	읽기 전용	프로토콜별 라이선스 확인
/api/cluster/nodes	읽기 전용	플랫폼 유형 검색
/api/security/accounts	읽기 전용	권한 발견
/api/security/roles	읽기 전용	권한 발견
/api/storage/aggregates	읽기 전용	데이터 저장소/볼륨 프로비저닝 중 애그리게이트 공간 확인
/api/storage/cluster	읽기 전용	클러스터 수준의 공간 및 효율성 데이터를 얻으려면
/api/storage/disks	읽기 전용	집합체에 연결된 디스크를 얻으려면
/api/storage/qos/policies	읽기/생성/수정	QoS 및 VM 정책 관리

/api/svm/svms	읽기 전용	클러스터가 로컬에 추가될 때 SVM 구성을 가져오려면.
/api/network/ip/interfaces	읽기 전용	스토리지 백엔드 추가 - 관리 LIF 범위가 클러스터/SVM임을 식별합니다.
/api/storage/availability-zones	읽기 전용	SAZ 검색. ONTAP 9.16.1 릴리스 이상 및 ASA r2 시스템에 적용됩니다.
/api/cluster/metrocluster	읽기 전용	MetroCluster 상태 및 구성 세부 정보를 가져옵니다.

VMware vSphere ONTAP API 기반 클러스터 범위 사용자를 위한 **ONTAP tools for VMware vSphere** 생성

데이터 저장소에 대한 PATCH 작업 및 자동 롤백을 수행하려면 검색, 생성, 수정 및 삭제 권한이 필요합니다. 이러한 권한이 없으면 워크플로 및 정리 작업에 문제가 발생할 수 있습니다.

검색, 생성, 수정 및 삭제 권한을 가진 ONTAP API 기반 사용자는 ONTAP tools 워크플로를 관리할 수 있습니다.

위에 언급된 모든 권한을 가진 클러스터 범위 사용자를 생성하려면 다음 명령을 실행하십시오.

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all
```

```
security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly
```

```
security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
```

```
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

또한 ONTAP 버전 9.16.0 이상에서는 다음 명령을 실행하십시오.

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

ONTAP 버전 9.16.1 이상의 ASA r2 시스템의 경우 다음 명령을 실행하십시오.

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

VMware vSphere ONTAP API 기반 **SVM** 범위 사용자를 위한 **ONTAP tools for VMware vSphere** 생성

모든 Privileges을 가진 SVM 범위 사용자를 생성하려면 다음 명령을 실행하십시오.

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

또한 ONTAP 버전 9.16.0 이상에서는 다음 명령을 실행하십시오.

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

이전에 생성한 API 기반 역할을 사용하여 새 API 기반 사용자를 생성하려면 다음 명령을 실행하십시오.

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

예:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

다음 명령을 실행하여 계정 잠금을 해제하고 관리 인터페이스 액세스를 활성화하십시오.

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

예:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

ONTAP tools for VMware vSphere 10.1 사용자를 10.3 사용자로 업그레이드

JSON 파일을 사용하여 클러스터 범위 사용자를 생성한 ONTAP tools for VMware vSphere 10.1 사용자는 user admin 권한으로 다음 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드하십시오.

제품 기능 관련:

- VSC
- VSC 및 VASA Provider
- VSC와 SRA
- VSC, VASA Provider 및 SRA.

클러스터 권한:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

JSON 파일을 사용하여 SVM 범위 사용자를 생성한 ONTAP tools for VMware vSphere 10.1 사용자는 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.3 릴리스로 업그레이드하십시오.

SVM 권한:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

-vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

다음 명령을 활성화하려면 기존 역할에 *vserver nvme namespace show* 및 *vserver nvme subsystem show* 명령을 추가하십시오.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

ONTAP tools for VMware vSphere 10.3 사용자를 10.4 사용자로 업그레이드

ONTAP 9.16.1부터 ONTAP tools for VMware vSphere 10.3 사용자를 10.4 사용자로 업그레이드하십시오.

JSON 파일을 사용하여 클러스터 범위 사용자를 생성하고 ONTAP 버전 9.16.1 이상인 ONTAP tools for VMware vSphere 10.3 사용자는 관리자 권한으로 ONTAP CLI 명령을 사용하여 10.4 릴리스로 업그레이드하십시오.

제품 기능 관련:

- VSC
- VSC 및 VASA Provider
- VSC와 SRA
- VSC, VASA Provider 및 SRA.

클러스터 권한:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

ONTAP tools에 스토리지 백엔드 추가

ONTAP tools for VMware vSphere를 사용하여 ESXi 호스트의 스토리지 백엔드를 추가하고 관리할 수 있습니다. 클러스터 또는 SVM을 온보딩하고, MetroCluster 지원을 활성화하고, 안전한 연결을 위한 인증서를 검증할 수 있습니다. ONTAP tools Manager 또는 vSphere 클라이언트를 사용하여 스토리지 백엔드를 구성하고, 인증서 상태를 모니터링하고, 클러스터 변경 후 리소스를 수동으로 다시 검색할 수 있습니다.

로컬에 스토리지 백엔드를 추가하려면 ONTAP tools 인터페이스에서 클러스터 또는 SVM 자격 증명을 사용하십시오. 로컬 스토리지 백엔드는 선택한 vCenter Server에서만 사용할 수 있습니다. ONTAP tools는 vVols 또는 VMFS 데이터스토어 관리를 위해 SVM을 vCenter Server에 매핑합니다. VMFS 데이터스토어 및 SRA 워크플로우의 경우, 클러스터를 전역적으로 매핑하지 않고 SVM 자격 증명을 사용할 수 있습니다.

글로벌 스토리지 백엔드를 추가하려면 ONTAP tools Manager에서 ONTAP 클러스터 자격 증명을 사용하십시오. 글로벌 스토리지 백엔드를 사용하면 vVol 관리에 필요한 클러스터 리소스를 식별하는 검색 워크플로를 수행할 수 있습니다. 멀티테넌트 환경에서는 SVM 사용자를 로컬에 추가하여 vVols 데이터스토어를 관리할 수 있습니다.

글로벌 및 로컬 스토리지 백엔드에 대한 자세한 내용은 KB 문서 "OTV 10: 스토리지 백엔드 글로벌 및 로컬 범위란 무엇인가"를 참조하십시오.

MetroCluster 지원이 ONTAP에서 활성화된 경우 소스 및 대상 클러스터를 로컬 또는 글로벌 스토리지 백엔드로 온보딩하십시오.

시작하기 전에

인증서에 유효한 SAN(Subject Alternative Name) 필드가 포함되어 있는지 확인하십시오. ONTAP 시스템은 SAN 필드를 사용하여 클러스터 및 SVM 관리 LIF를 식별합니다.

ONTAP tools Manager 사용

멀티테넌트 환경에서는 스토리지 백엔드 클러스터를 전역적으로 추가하고 SVM을 로컬로 추가하여 SVM 사용자 자격 증명을 사용할 수 있습니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소 또는 FQDN, 사용자 이름 및 비밀번호 정보를 제공하십시오.

   IPv4 및 IPv6 주소 관리 LIF가 지원됩니다.

5. ONTAP 클러스터 인증서를 자동으로 가져와서 승인하거나, 인증서 위치를 찾아 수동으로 업로드할 수 있습니다.

   필요한 경우 유지 관리 콘솔에서 SAN(Subject Alternative Name) 유효성 검사를 비활성화할 수 있습니다. 자세한 내용은 "인증서 유효성 검사 플래그 변경"을 참조하십시오.

6. 추가하는 스토리지 백엔드가 MetroCluster 구성의 일부인 경우, ONTAP Tools Manager에 피어링된 클러스터를 추가하라는 팝업 메시지가 표시됩니다. *추가*를 선택하고 MetroCluster 피어 스토리지 백엔드에 대한 세부 정보를 입력하십시오.

   ONTAP 시스템이 전환 및 스위치백을 수행한 후 ONTAP tools 검색을 수동으로 실행하십시오.

vSphere 클라이언트 사용자 인터페이스 사용

vVols 데이터스토어는 vSphere 클라이언트 사용자 인터페이스를 통한 SVM 사용자의 직접 추가를 지원하지 않습니다.

1. vSphere 클라이언트에 로그인합니다.
2. 바로가기 페이지에서 플러그인 섹션 아래에 있는 *NetApp ONTAP tools*를 선택합니다.
3. 사이드바에서 *스토리지 백엔드*를 선택합니다.
4. 스토리지 백엔드를 추가하고 서버 IP 주소, 사용자 이름, 비밀번호 및 포트 정보를 제공하십시오.

   클러스터 기반 자격 증명과 IPv4 또는 IPv6 관리 LIF를 사용하여 스토리지 백엔드를 추가할 수 있습니다. SVM 사용자를 직접 추가하려면 SVM 기반 자격 증명과 SVM 관리 LIF를 제공하십시오. 클러스터가 이미 온보딩된 경우 해당 클러스터에서 SVM 사용자를 다시 온보딩할 수 없습니다.

5. ONTAP 클러스터 인증서를 자동으로 가져와서 승인하거나, 인증서 위치를 찾아 수동으로 업로드할 수 있습니다.
6. 추가된 스토리지 백엔드가 MetroCluster 구성의 일부인 경우, ONTAP tools는 **MetroCluster** 피어 추가

화면을 표시합니다. 피어 스토리지 백엔드를 추가하려면 *피어 추가*를 선택하십시오.

ONTAP 시스템이 전환 및 스위치백을 수행한 후 ONTAP tools 검색을 수동으로 실행하십시오.

ONTAP tools는 스토리지 백엔드 페이지에 새로 추가된 스토리지 백엔드를 나열합니다. 인증서가 30일 이내에 만료되는 경우, ONTAP tools는 인증서 만료일 열에 경고를 표시합니다. 만료 후에 ONTAP tools는 스토리지 시스템에 연결할 수 없기 때문에 스토리지 백엔드를 알 수 없음으로 표시합니다.

관련 정보

"OTV 10: 스토리지 백엔드 글로벌 및 로컬 범위란 무엇인가"

"클러스터를 MetroCluster 구성으로 설정"

ONTAP 도구에서 스토리지 백엔드를 vCenter Server 인스턴스에 연결합니다

vCenter Server 인스턴스와 스토리지 백엔드를 연결하여 모든 vCenter Server 인스턴스에서 액세스할 수 있도록 하십시오. MetroCluster 구성의 경우, 스토리지 백엔드 클러스터를 연결할 때 해당 피어 클러스터도 vCenter Server와 연결해야 합니다.

단계

1. 웹 브라우저에서 ONTAP tools Manager를 실행합니다.
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 배포 중에 제공한 ONTAP tools for VMware vSphere 관리자 자격 증명으로 로그인하십시오.
3. 사이드바에서 vCenter를 선택합니다.
4. 스토리지 백엔드에 연결하려는 vCenter Server 인스턴스 옆에 있는 세로 점 세 개(…)를 선택합니다.
5. 드롭다운 메뉴에서 선택한 vCenter Server 인스턴스와 연결할 스토리지 백엔드를 선택합니다.

ONTAP 도구에서 네트워크 액세스 구성

기본적으로 ESXi 호스트에서 검색된 모든 IP 주소는 네트워크 액세스를 구성하지 않는 한 내보내기 정책에 자동으로 추가됩니다. 특정 IP 주소에서만 액세스를 허용하도록 내보내기 정책을 수정할 수 있습니다. 제외된 ESXi 호스트가 마운트 작업을 시도하면 작업이 실패합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 플러그인 섹션의 바로가기 페이지에서 *NetApp ONTAP tools*를 선택하십시오.
3. ONTAP tools의 왼쪽 창에서 설정 > 네트워크 액세스 관리 > *편집*으로 이동합니다.

   여러 IP 주소를 추가하려면 쉼표, 범위, CIDR(Classless Inter-Domain Routing) 또는 이 세 가지를 모두 조합하여 목록을 구분하십시오.

4. *저장*을 선택합니다.

ONTAP tools에서 데이터 저장소를 생성합니다

호스트 클러스터 수준에서 데이터 저장소를 생성하면 ONTAP tools는 해당 데이터 저장소를 모든 대상 호스트에 마운트하고 필요한 권한이 있는 경우에만 작업을 활성화합니다.

기본 데이터 저장소와 **vCenter Server** 및 **ONTAP tools**로 관리되는 데이터 저장소 간의 상호 운용성

ONTAP tools for VMware vSphere 10.4부터 ONTAP tools는 데이터스토어에 대한 중첩 igroup을 생성합니다. 상위 igroup은 데이터스토어에 특화되고 하위 igroup은 호스트에 매핑됩니다. ONTAP System Manager에서 플랫 igroup을 생성하고 이를 사용하여 ONTAP tools를 사용하지 않고도 VMFS 데이터스토어를 생성할 수 있습니다. 자세한 내용은 "SAN 이니시에이터 및 igroup 관리"을 참조하십시오.

스토리지를 온보딩하고 데이터스토어 검색을 실행하면 ONTAP tools가 VMFS 데이터스토어의 플랫 igroup을 중첩 igroup으로 변경합니다. 이전의 플랫 igroup을 사용하여 새 데이터스토어를 생성할 수 없습니다. 중첩 igroup을 재사용하려면 ONTAP tools 인터페이스 또는 REST API를 사용하십시오.

vVols 데이터스토어를 생성합니다**.**

ONTAP tools for VMware vSphere 10.3부터 ASA r2 시스템에서 공간 효율성을 thin으로 설정하여 vVols 데이터스토어를 생성할 수 있습니다.vVol. VASA Provider는 vVol 데이터스토어를 생성하는 동안 컨테이너와 원하는 프로토콜 엔드포인트를 생성합니다. VASA Provider는 이 컨테이너에 백업 볼륨을 할당하지 않습니다.

시작하기 전에

- 루트 애그리게이트가 SVM에 매핑되지 않도록 하십시오.
- VASA Provider가 선택한 vCenter에 등록되어 있는지 확인하십시오.
- ASA r2 스토리지 시스템에서 SVM은 SVM 사용자를 위해 애그리게이트에 매핑되어야 합니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 선택합니다.
3. *데이터 저장소 유형*으로 vVols를 선택합니다.
4. 데이터 저장소 이름*과 *프로토콜 정보를 입력하십시오.

   ASA r2 시스템은 vVols에 대해 iSCSI 및 FC 프로토콜을 지원합니다.

5. 데이터스토어를 생성할 스토리지 VM을 선택합니다.
6. 고급 옵션에서:
   - *사용자 지정 내보내기 정책*을 선택하는 경우 모든 개체에 대해 vCenter에서 검색을 실행해야 합니다. 이 옵션은 사용하지 않는 것이 좋습니다.
   - iSCSI 및 FC 프로토콜에 대해 **Custom initiator group** 이름을 선택할 수 있습니다.

   ASA r2 스토리지 시스템 유형 SVM에서는 데이터 저장소가 논리적 컨테이너일 뿐이므로 스토리지 유닛(LUN/네임스페이스)이 생성되지 않습니다.

7. 저장소 속성 창에서 새 볼륨을 생성하거나 기존 볼륨을 사용할 수 있습니다. 하지만 이 두 가지 유형의 볼륨을 결합하여 vVols 데이터스토어를 생성할 수는 없습니다.

   새 볼륨을 생성할 때 데이터스토어에서 QoS를 활성화할 수 있습니다. 기본적으로 LUN 생성 요청마다 하나의 볼륨이 생성됩니다. ASA r2 스토리지 시스템의 vVols 데이터스토어의 경우 이 단계를 건너뛸 수 있습니다.

8. 요약 창에서 선택 내용을 검토하고 *완료*를 선택하십시오.

NFS 데이터스토어 생성

NFS 데이터스토어는 NFS 프로토콜을 사용하여 ESXi 호스트를 공유 스토리지에 연결합니다. 간단하고 유연하며 VMware vSphere 환경에서 사용됩니다.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 선택합니다.

3. 데이터 저장소 유형 필드에서 NFS를 선택합니다.
4. 이름 및 프로토콜 창에 데이터 저장소 이름, 크기 및 프로토콜 정보를 입력합니다. 고급 옵션에서 *데이터 저장소 클러스터*와 *Kerberos 인증*을 선택합니다.

   Kerberos 인증은 NFS 4.1 프로토콜이 선택된 경우에만 사용할 수 있습니다.

5. 스토리지 창에서 플랫폼 및 스토리지 **VM** 을 선택합니다.
6. 고급 옵션에서 *사용자 지정 내보내기 정책*을 선택하면 모든 개체에 대해 vCenter에서 검색을 실행합니다. 이 옵션은 사용하지 않는 것이 좋습니다.

   SVM의 기본 볼륨 정책 또는 루트 볼륨 정책을 사용하여 NFS 데이터스토어를 생성할 수 없습니다.

   - 고급 옵션에서 비대칭 토글 버튼은 플랫폼 드롭다운 메뉴에서 성능 또는 용량이 선택된 경우에만 표시됩니다.
   - 플랫폼 드롭다운 메뉴에서 모두 옵션을 선택하면 vCenter의 모든 SVM을 볼 수 있습니다. 플랫폼 및 비대칭 플래그는 가시성에 영향을 미치지 않습니다.
7. 저장소 속성 창에서 볼륨 생성을 위한 애그리게이트를 선택합니다. 고급 옵션에서 필요에 따라 공간 예약 및 *QoS 활성화*를 선택합니다.
8. 요약 창에서 선택 사항을 검토하고 완료를 선택하십시오.

ONTAP tools는 NFS 데이터스토어를 생성하고 모든 호스트에 마운트합니다.

VMFS 데이터스토어 생성

VMFS는 가상 머신 파일을 저장하는 클러스터형 파일 시스템입니다. 여러 ESXi 호스트가 vMotion 및 고가용성 기능을 위해 동일한 VM 파일에 동시에 액세스할 수 있습니다.

보호된 클러스터에서:

- VMFS 데이터스토어만 생성할 수 있습니다. 보호된 클러스터에 VMFS 데이터스토어를 추가하면 자동으로 보호됩니다.
- 보호된 호스트 클러스터가 하나 이상 있는 데이터 센터에는 데이터 저장소를 생성할 수 없습니다.
- 상위 호스트 클러스터가 "자동 장애 조치 이중화 정책"(균일 또는 비균일 구성)으로 보호되는 경우 ESXi 호스트에 데이터 저장소를 생성할 수 없습니다.
- VMFS 데이터스토어는 비동기 관계로 보호되는 ESXi 호스트에만 생성할 수 있습니다. "자동 장애 조치 이중화" 정책으로 보호되는 호스트 클러스터의 일부인 ESXi 호스트에는 데이터스토어를 생성하고 마운트할 수 없습니다.

시작하기 전에

- ONTAP 스토리지 측에서 각 프로토콜에 대한 서비스 및 LIF를 활성화하십시오.
- ASA r2 스토리지 시스템의 SVM 사용자를 위해 SVM을 애그리게이트에 매핑합니다.
- NVMe/TCP 프로토콜을 사용하는 경우 ESXi 호스트를 구성하십시오.
  a. 검토 "VMware 호환성 가이드"

VMware vSphere 7.0 U3 이상 버전은 NVMe/TCP 프로토콜을 지원합니다. 하지만 VMware vSphere 8.0 이상 버전을 사용하는 것이 좋습니다.

b. 네트워크 인터페이스 카드(NIC) 공급업체가 NVMe/TCP 프로토콜을 사용하는 ESXi NIC를 지원하는지 확인하십시오.

c. NIC 공급업체 사양에 따라 ESXi NIC를 NVMe/TCP용으로 설정하십시오.

d. VMware vSphere 7 릴리스를 사용하는 경우 VMware 사이트 "NVMe over TCP 어댑터에 대한 VMkernel 바인딩 구성"의 지침에 따라 NVMe/TCP 포트 바인딩을 구성하십시오. VMware vSphere 8 릴리스를 사용하는 경우 "ESXi에서 TCP를 통한 NVMe 구성"에 따라 NVMe/TCP 포트 바인딩을 구성하십시오.

e. VMware vSphere 7 릴리스의 경우, NVMe/TCP 소프트웨어 어댑터를 구성하려면 페이지 "NVMe over RDMA 또는 NVMe over TCP 소프트웨어 어댑터 활성화"의 지침을 따르십시오. VMware vSphere 8 릴리스의 경우, NVMe/TCP 소프트웨어 어댑터를 구성하려면 "RDMA를 통한 소프트웨어 NVMe 또는 TCP를 통한 NVMe 어댑터 추가"을 따르십시오.

f. ESXi 호스트에서 "스토리지 시스템 및 호스트 검색" 작업을 실행하십시오. 자세한 내용은 "vSphere 8.0 업데이트 1 및 ONTAP 9.13.1을 사용하여 VMFS 데이터스토어에 NVMe/TCP를 구성하는 방법"을 참조하십시오.

- NVME/FC 프로토콜을 사용하는 경우 다음 단계를 수행하여 ESXi 호스트를 구성하십시오.

a. 아직 활성화하지 않았다면 ESXi 호스트에서 NVMe over Fabrics(NVMe-oF)를 활성화하십시오.

b. SCSI 조닝을 완료합니다.

c. ESXi 호스트와 ONTAP 시스템이 물리적 및 논리적 계층에서 연결되어 있는지 확인하십시오.

FC 프로토콜용 ONTAP SVM을 구성하려면 다음을 참조하십시오. "FC용 SVM 구성"

VMware vSphere 8.0에서 NVMe/FC 프로토콜을 사용하는 방법에 대한 자세한 내용은 "ESXi 8.x with ONTAP에 대한 NVMe-oF 호스트 구성"를 참조하십시오.

VMware vSphere 7.0에서 NVMe/FC를 사용하는 방법에 대한 자세한 내용은 "ONTAP NVMe/FC 호스트 구성 가이드" 및 "TR-4684"을 참조하십시오.

단계

1. vSphere 클라이언트에 로그인합니다.
2. 호스트 시스템, 호스트 클러스터 또는 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **NetApp ONTAP tools** > *데이터 저장소 생성*을 선택합니다.
3. VMFS 데이터 저장소 유형을 선택합니다.
4. 이름 및 프로토콜 창에 데이터스토어 이름, 크기 및 프로토콜 정보를 입력합니다. 기존 VMFS 클러스터에 새 데이터스토어를 추가하려면 고급 옵션에서 데이터스토어 클러스터를 선택합니다.
5. **Storage** 창에서 스토리지 VM을 선택합니다. 필요에 따라 고급 옵션 섹션에서 *사용자 지정 이니시에이터 그룹 이름*을 입력합니다. 데이터스토어에 대해 기존 igroup을 선택하거나 사용자 지정 이름으로 새 igroup을 생성할 수 있습니다.

   NVMe/FC 또는 NVMe/TCP 프로토콜을 선택하면 새 네임스페이스 서브시스템이 생성되어 네임스페이스 매핑에 사용됩니다. ONTAP tools는 데이터스토어 이름을 포함하는 자동 생성된 이름을 사용하여 네임스페이스 서브시스템을 생성합니다. **Storage** 창의 고급 옵션에 있는 **custom namespace subsystem name** 필드에서 네임스페이스 서브시스템의 이름을 변경할 수 있습니다.

6. 스토리지 속성 창에서:

   a. 드롭다운 옵션에서 *Aggregate*를 선택합니다.

      ASA r2 스토리지 시스템의 경우 스토리지가 분산되어 있으므로 집계**(Aggregate)** 옵션이 표시되지 않습니다. ASA r2 스토리지 시스템 유형으로 SVM을 선택하면 스토리지 속성 페이지에 QoS 활성화 옵션이 표시됩니다.

   b. ONTAP tools는 선택한 프로토콜을 기반으로 씬 스페이스 예약이 있는 스토리지 단위(LUN/Namespace)를 생성합니다.

      ONTAP 9.16.1 버전부터 ASA r2 스토리지 시스템은 클러스터당 최대 12개의 노드를 지원합니다.

   c. 이기종 클러스터인 12노드 SVM을 사용하는 ASA r2 스토리지 시스템에 대해 *성능 서비스 수준*을 선택하십시오. 선택한 SVM이 동종 클러스터이거나 SVM 사용자를 사용하는 경우에는 이 옵션을 사용할 수 없습니다.

      'Any'는 기본 성능 서비스 수준(PSL) 값입니다. 이 설정은 ONTAP 균형 배치 알고리즘을 사용하여 스토리지 유닛을 생성합니다. 하지만 필요에 따라 성능 또는 익스트림 옵션을 선택할 수 있습니다.

   d. 필요에 따라 기존 볼륨 사용 및 **QoS** 활성화 옵션을 선택하고 세부 정보를 입력하십시오.

      ASA r2 스토리지 유형에서는 볼륨 생성 또는 선택이 스토리지 유닛 생성(LUN/네임스페이스)에 적용되지 않습니다. 따라서 이러한 옵션은 표시되지 않습니다.

   기존 볼륨을 사용하여 NVMe/FC 또는 NVMe/TCP 프로토콜을 사용하는 VMFS 데이터스토어를 생성할 수 없습니다. VMFS 데이터스토어를 위한 새 볼륨을 생성하십시오.

7. 요약 창에서 데이터 저장소 세부 정보를 검토하고 *완료*를 선택합니다.

   보호된 클러스터에 데이터 저장소를 생성하면 "The datastore is being mounted on a protected Cluster."라는 읽기 전용 메시지가 표시될 수 있습니다.

결과

ONTAP tools는 VMFS 데이터스토어를 생성하고 모든 호스트에 마운트합니다.